# Special Issues
# Upcoming Special Issue on Socio-Technical Ecosystem Considerations: Threats and Opportunities for AI in Cybersecurity

The *IEEE Transactions on Technology and Society* has launched a call for papers for an upcoming special issue with a closing date of 01 February 2022.

## Description

New technology development and adoption of those new technologies continues to accelerate. We live today in a saturated, information environment with unprecedented dependence on digital technologies.

An element of the expansion of digital technologies is a shift in Artificial Intelligence (AI) technology from research laboratories into the hands of anyone with a smartphone [1]. AI powered search, personalization and automation are being deployed across sectors, from education to healthcare, to policing, to finance. Wide AI diffusion is then reshaping the way organizations, communities and individuals' function. [2].

The potentially radical consequences of AI have pushed nation states across the globe to publish strategies on how they seek to shape, drive and leverage the disruptive capabilities offered by AI technologies to bolster their prosperity and security [3].
In the context of new partnerships, and within existing alliances, these efforts can be seen as an opportunity for positive alignment so that governance and new capabilities create value for citizens' well-being, privacy [4] and safety [5]. Those same national efforts to lead, nurture and sustain AI to transform citizens' lives can also be viewed as a competition, or even as an international AI arm race undermining international stability [6].

Within the intelligence alliance of Five Eyes countries, policy initiatives for the governance of AI in the security and defense domains focus on potential security breaches, economic consequences, and political threats [7]. The relative disregard for social and environmental factors is problematic. This lack of attention may shape how AI could be used in cybersecurity for harm, beyond the organizational level, and systems of governance that may or may not respect the rule of law [8]. Furthermore, AI systems themselves introduce new targets for malicious actors.

There has been a resurgence within academia and associated specialist scientific institutes to investigate socio-technical factors (i.e., the interaction of people, tasks,

structure, and technology) shaping cybersecurity. But there has still been limited focus on the complex external environment and dynamic socio-cyber-physical ecosystem [9].

The vast majority of security research relates to the traditional Confidentiality-Integrity-Availability (CIA) triad. While this strategy has continued to strengthen organizational and infrastructural defenses, we must consider the new emergent threats. These include: homogeneity in products at their core operating system, large storage area network providers and critical telecommunication exchanges and international banking interchanges, and the supply of electricity and water and the respective interdependencies therein [10]. Of particular importance are autonomous systems leveraging advanced machine learning systems that incorporate blackbox models (e.g., billion parameter neural networks), and highly complex technologies that may be microscopic and even embeddable and undetectable [11].

The socio-technical approach [12] is promising in this context, as it allows us to move beyond a particular system of interest and associated inputs, outputs and attack vectors to an open systems environment, at the heart of which is stakeholder centricity [13].

This special issue invites research focused on a deeper examination of value chain stakeholders [14], their roles and responsibilities and their corresponding dynamic interactions and interdependencies in the present turbulent environment [15]. Contributions to the special issue will focus a range of questions. For example, how do different federal and state laws, regulations, policies, guidelines and economic infrastructure shape the AI and cybersecurity landscape in an international context? How is AI and cybersecurity being applied as a potential global offset? How can cybersecurity specialists respond to these threats once they have been explicitly identified?

*To this end, this special issue aims to bring together researchers from different disciplines exploring the intersections of socio-technical imaginaries, ethics, and the role of AI in cybersecurity as an exemplary crisis for inquiry and debate.*

## Important dates

- Submissions open: Now
- Submissions close: 1 February 2022
- Publication of final issue: 1 September 2022
- Please note, TTS subscribes to Pre-Print model of access. Once your paper is accepted it will appear online freely available with DOI until it is placed in the special issue in September 2022.

## Topics

Submissions are especially invited on, but not limited to, the following topics intersecting with AI and/in Cybersecurity:

- Responsible innovation and science and technology ethics [16, 17]
- Science and technology policy, regulation, and governance [18]
- Public understanding of and engagement with AI and cybersecurity [19]
- Innovation processes [20, 21]
- Algorithmic and technological biases and inequalities [22]
- Impacts of AI and cybersecurity unleashed by nation states
- Impacts of AI and cybersecurity on nascent wearable and implantable technologies [23, 24, 25, 26]
- Socio-technical imaginaries, power, discrimination, contradiction [27, 28, 29]
- Anticipatory/futures-literate approaches to the future of AI and cyber security [30]
- The security of AI algorithms in a socio-technical context [31]
- The role of scenarios, vignettes, stories and qualitative approaches to AI and cybersecurity understanding [32, 33]
- Data/AI-driven cybersecurity for attack and defense [34]
- Intelligence challenges related to AI and cybersecurity [35]
- Holistic and exploratory approaches to AI- big picture national perspectives
- Public interest technologies in AI and cybersecurity [36]
- The role of regulation and or (soft)/laws on the future practices of AI, considering both national (e.g. governance of AI) and international (AI for defense) perspectives [37, 38]
- The role of education and training in raising societal awareness of cybersecurity threats [39, 40]
- Opportunities and challenges for socio-technical systems enhancement [41]

Submissions that will be considered out of scope include:

- Work that does not address ethical or societal or environmental impacts of AI and/in cybersecurity
- Formal methods research where a thematically targeted engineering journal would be more appropriate (e.g. in the field of signal processing or artificial intelligence or security)

## How to Submit

For article formats, templates, and submission information, see

Submit your papers through https://ieee.atyponrex.com/dashboard/?journalCode=TTS .

### Review and publication process

Papers will be reviewed and published online first upon acceptance on a rolling basis.

Papers accepted for full review will be reviewed by two anonymous reviewers and a meta-reviewer, with a target turnaround of three weeks for a review decision.

To be considered for the special issue, revisions of papers that are revise-and-resubmit or accepted with minor/major changes need to be submitted before 1st June 2022. Should they require a further cycle of revision, they will be included in a future regular issue of the Transactions.

### Guest Editors

**Mariarosaria Taddeo**, Oxford Internet Institute, University of Oxford, UK and Turing Fellow, Alan Turing Institute, UK

**Paul Jones**, National Cyber Security Center, UK

**Roba Abbas**, School of Business, University of Wollongong, Australia

**Kathleen Vogel**, School for the Future of Innovation in Society, Arizona State University, USA

### Bibliography

[1] Gil, Y. and Selman, B. August 6, 2019, *A 20-Year Community Roadmap for Artificial Intelligence Research in the US. Computing Community Consortium (CCC) and Association for the Advancement of Artificial Intelligence (AAAI)*. https://arxiv.org/ftp/arxiv/papers/1908/1908.02624.pdf

[2] UK Government, 21 May 2019, "AI Sectoral Deal", *Gov.UK*, https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal

[3] Select Committee on Artificial Intelligence of the National Science and Technology Council, June 2019, "The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update (nitrd.gov)", *Executive Office of the President*, https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf

[4] Michael, K., Kobran, S., Abbas, R. and Hamdoun, S., 2019, "Privacy, Data Rights and Cybersecurity: Technology for Good in the Achievement of Sustainable Development Goals," *2019 IEEE International Symposium on Technology and Society (ISTAS)*, 1-13.

[5] Michael, K. and Abbas, R., 13 March 2020, "Responsible AI: Ensuring Reliable, Safe & Trustworthy Systems", *The Thirteenth Workshop on the Social Implications of National Security (SINS20)*, Human Factors Series, Arizona State University, Washington DC, USA, https://www.katinamichael.com/sins20

[6] Michael, K., Roba Abbas, Jeremy Pitt, 24 May 2021, "Maintaining Control over AI", *Issues in Science and Technology: Forum*, XXXVII(3), Spring 2021, https://issues.org/debating-human-control-over-artificial-intelligence-forum-shneiderman/

[7] Helen L. 24 July 2020, A sociotechnical approach to cyber security: How a multi-disciplinary approach can help us deliver security that works in the real world, *National Cyber Security Centre*, https://www.ncsc.gov.uk/blog-post/a-sociotechnical-approach-to-cyber-security

[8] Davis, Matthew C. and Rose Challenger, Dharshana N.W. Jayewardene, Chris W. Clegg, "Advancing socio-technical systems thinking: A call for bravery", *Applied Ergonomics*, Vol. 45, Iss. 2, Part A, 2014, pp. 171-180, https://doi.org/10.1016/j.apergo.2013.02.009

[9] Abbas, Roba and Katina Michael, 10 August 2020, "The Design and Implementation of the COVIDSafe App in Australia: A Socio-Technical Overview", *International COVID-19 Congress*, IEEE Bangladesh Section, Dhaka, Bangladesh, https://www.katinamichael.com/seminars/2020/8/10/the-design-and-implementation-of-the-covidsafe-app-in-australia

[10] Stephan, K.D., K. Michael, M. G. Michael, L. Jacob and E. P. Anesta, 2012, "Social Implications of Technology: The Past, the Present, and the Future," in *Proceedings of the IEEE*, 100, (no. Special Centennial Issue): 1752-1781, 13 May 2012, doi: 10.1109/JPROC.2012.2189919.

[11] CCC, 27 October 2020, "Assured Autonomy: Path Toward Living With Autonomous Systems We Can Trust", *Community, Computing, Consortium: Catalyst*, Phoenix, Arizona, https://cra.org/ccc/wp-content/uploads/sites/2/2020/10/Assured-Autonomy-Workshop-Report-Final.pdf

[12] Bostrom, Robert P., and J. Stephen Heinen. 1977, "MIS Problems and Failures: A Socio-Technical Perspective, Part II: The Application of Socio-Technical Theory," *MIS Quarterly*, 1(4): 11–28.

[13] Pitt, J. and J. Ober, "Democracy by Design: Basic Democracy and the Self-Organization of Collective Governance," *2018 IEEE 12th International Conference on Self-Adaptive and Self-Organizing Systems (SASO)*, 20-29, doi: 10.1109/SASO.2018.00013.

[14] Carayon P. Human factors of complex sociotechnical systems. *Appl Ergon*. 2006 Jul;3 7(4):525-35. doi: 10.1016/j.apergo.2006.04.011

[15] Carayannis, E.G., Rakhmatullin, R., 2014, "The Quadruple/Quintuple Innovation Helixes and Smart Specialization Strategies for Sustainable and Inclusive Growth in Europe and Beyond", *J Knowl Econ*, 5: 212–239.

[16] European Parliament, March 2020, "The ethics of artificial intelligence: Issues and initiatives", *European Parliament, Panel for the Future of Science and Technology*, EPRS | European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 634.452, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf

[17] Vogel, K., Balmer, B., Weiss, S., Kroener, I., Matsumoto, M. and Brian, R., 2016. *The Handbook of Science and Technology Studies*, pp.973-1002.

[18] Pitt, J., J. Dryzek and J. Ober, "Algorithmic Reflexive Governance for Socio-Techno-Ecological Systems," *in IEEE Technology and Society Magazine*, 39(2): 52-59, June 2020, doi: 10.1109/MTS.2020.2991500.

[19] Michael, Katina and Roba Abbas, 10 August 2020, "Lessons from COVIDSafe: Toward Public Interest Technologies of the Future", *International COVID-19 Congress*, IEEE Bangladesh Section, Dhaka, Bangladesh, https://www.katinamichael.com/seminars/2020/8/10/lessons-from-covidsafe-toward-public-interest-technologies-of-the-future

[20] Ellul, Jacques. 1962, "The technological order." *Technology and Culture*, 3(4): 394-421.

[21] Geels, F.W., 2002. Technological transitions as evolutionary reconfiguration processes: a multi-level perspective and a case-study. *Research policy*, 31(8-9), pp.1257-1274.

[22] Mittelstadt, B.D., Allo, P., Taddeo, M., Wachter, S. and Floridi, L., 2016. The ethics of algorithms: Mapping the debate. *Big Data & Society* 3, 2: 205395171667967.

[23] Perusco, L. and K. Michael, 2007, "Control, trust, privacy, and security: evaluating location-based services," in *IEEE Technology and Society Magazine*, 26(1): 4-16, Spring 2007, doi: 10.1109/MTAS.2007.335564.

[24] Gokye, Deniz and Katina Michael, Digital Wearability Scenarios: Trialability on the run, *IEEE Consumer Electronics Magazine*, Year: 2015, Volume: 4, Issue: 2, pp. 82-91, DOI: 10.1109/MCE.2015.2393005

[25] Johnson, B.D., 2010, November. Science Fiction for Scientists!! An Introduction to SF Prototypes and Brain Machines. In *Intelligent Environments (Workshops)* (pp. 195-203).
[26] Michael, Katina, "DARPA's ADAPTER Program: Applying the ELSI Approach to a Semi-Autonomous Complex Socio-Technical System", *The Third 21st Century Wiener Conference*, Anna University, Chennai, India, 23-25 July 2021, pp. 1-10.
[27] Jasanoff, S. and Kim, S.H., 2013. Sociotechnical imaginaries and national energy policies. *Science as culture*, 22(2), pp.189-196.
[28] Jasanoff, S. and Kim, S.H., 2009. Containing the atom: Sociotechnical imaginaries and nuclear power in the United States and South Korea. *Minerva*, 47(2), p.119
[29] Sadowski, J. and Bendor, R., 2019. Selling smartness: Corporate narratives and the smart city as a sociotechnical imaginary. *Science, Technology, & Human Values*, 44(3), pp.540-563.
[30] Johnson, B.D., 2011. Science fiction prototyping: Designing the future with science fiction. *Synthesis Lectures on Computer Science*, 3(1), pp.1-190.
[31] Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M. and Floridi, L., 2018. Artificial intelligence and the 'good society': the US, EU, and UK approach. *Science and engineering ethics*, 24(2), pp.505-528.
[32] Abbas, R. 2021, "Socio-Technical Theory: The Role of Scenarios in Informing Design Choices. Threats and Opportunities for AI in Cybersecurity" in Kathleen Vogel and Katina Michael, *Workshop 2: Examining the Socio-Technical Ecosystem (STeS) Considerations*, The Alan Turing Institute, 26 February 2021.
[33] Lively, Genevieve, *Narratology*, Oxford University Press, 2019.
[34] Neil Dhir, Henrique Hoeltgebaum, Niall Adams, Mark Briers, Anthony Burke, Paul Jones, "Prospective Artificial Intelligence Approaches for Active Cyber Defense", April 20, 2021, https://arxiv.org/abs/2104.09981
[35] Taddeo, M., 2012. Information warfare: A philosophical perspective. *Philosophy & Technology*, 25(1), pp.105-120.
[36] Abbas, R., J. Pitt and K. Michael, "Socio-Technical Design for Public Interest Technology," in *IEEE Transactions on Technology and Society*, vol. 2, no. 2, pp. 55-61, June 2021, doi: 10.1109/TTS.2021.3086260. https://ieeexplore.ieee.org/document/9459499/
[37] Marchant, G.E., 2011. The growing gap between emerging technologies and the law. In *The growing gap between emerging technologies and legal-ethical oversight* (pp. 19-33). Springer, Dordrecht.
[38] Marchant, G.E., Abbot, K.W. and Allenby, B. eds., 2013. *Innovative governance models for emerging technologies*. Edward Elgar Publishing.
[39] Kohno, T. and Johnson, B.D., 2011, March. Science fiction prototyping and security education: cultivating contextual and societal thinking in computer security education and beyond. In *Proceedings of the 42nd ACM technical symposium on Computer science education* (pp. 9-14).
[40] Willis, S., Byrd, G. and Johnson, B.D., 2017. Challenge-based learning. *Computer*, 50(7), pp.13-16.
[41] Vogel, K.M., 2013. The need for greater multidisciplinary, sociotechnical analysis: The bioweapons case. *Studies in Intelligence*, 57(3), pp.1-10.